A Report
to the
Montana
Legislature

Information Systems Audit

Combined Healthcare Information and Montana Eligibility System for Medicaid

Department of Public Health and Human Services

February 2011

Legislative Audit
Division

10DP-07

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors
Angie Grove
Cindy Jorgenson

February 2011

The Legislative Audit Committee
of the Montana State Legislature:

This is our Information Systems audit of the Combined Healthcare Information and Montana Eligibility System (CHIMES) for Medicaid administered by the Department of Public Health and Human Services.

This report provides information about CHIMES – Medicaid and includes recommendations to strengthen system controls. Recommendations relate to managing user access, monitoring user activity, strengthening access security, better controlling system change migration, and strengthening data integrity.

We wish to express our appreciation to the department director and staff for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Department of Public Health and Human Services	Anna Whiting Sorrell, Director
	Laurie Lamson, Manager, Operations Services Branch
	Ron Baldwin, Chief Information Officer, Technology Services Division
	Hank Hudson, Manager, Economic Security Services Branch
	Linda Snedigar, Administrator, Human and Community Services Division
	Marie Matthews, Administrator, Business and Financial Services Division

MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION SYSTEMS

Combined Healthcare Information and Montana Eligibility System for Medicaid

Department of Public Health and Human Services

FEBRUARY 2011 10DP-07 REPORT SUMMARY

Montana Medicaid processes almost seven million medical claims every year at a cost of more than $775 million for health care services. The CHIMES-Medicaid system was implemented to assist in determining client eligibility.

Context

The Department of Public Health and Human Services (DPHHS) is responsible for managing Medicaid in Montana. One of the responsibilities of DPHHS is determining who is eligible to receive Medicaid coverage. To assist in the administration of Medicaid eligibility, DPHHS contracted with a third-party vendor to develop the Combined Healthcare Information and Montana Eligibility System (CHIMES) – Medicaid. CHIMES – Medicaid is a complex system with processing dictated by a wide variety of both state and federal statutes and regulations. In addition, CHIMES – Medicaid manages over 80,000 client eligibility records and interfaces with 27 other systems.

Because of the complexity and critical nature of the system, we conducted audit work regarding data integrity including data input, data processing, and system interfaces. Audit work also included a review of system security, management of changes to the system, and processes used during implementation of the system.

Results

We noted DPHHS followed industry standards when implementing CHIMES – Medicaid. We identified areas where controls could be strengthened. This report contains seven recommendations for improvement including:

- Actively managing user access
- Formally monitoring all user activity
- Ensuring compliance with password policy
- Strengthening access security
- Better controlling system change migration
- Ensuring security of access to system servers
- Strengthening data integrity

Recommendation Concurrence	
Concur	7
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

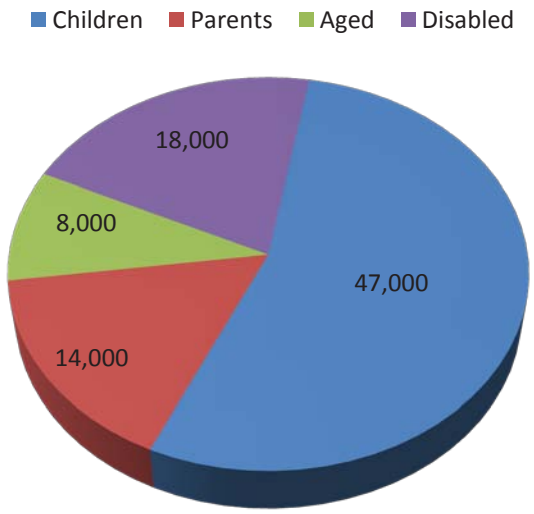
For a complete copy of the report or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to lad@mt.gov; or check the website at http://leg.mt.gov/audit.
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail lad@mt.gov.

Chapter I – Introduction and Background

Introduction

Medicaid is the third largest source of health insurance in the United States and covers approximately 12 percent of the total population. The Medicaid Insurance program resulted from the passage of Title XIX of the Social Security Act. Medicaid was created to provide health insurance for individuals and families with limited income and resources. Since its inception in 1965, Medicaid enrollment and expenditures have continued to expand.

Figure 1
Montana Medicaid: Clients Served



Source: Compiled by Legislative Audit Division.

According to Department of Public Health and Human Services (DPHHS) records, in Montana, Medicaid insures an average of almost 87,000 clients each month. A general breakdown of clients served is provided in Figure 1. Montana Medicaid processes almost 7 million medical claims every year at a cost of more than $775 million for health care services. The Medicaid program is jointly financed by the state and the federal government. In federal fiscal year 2008, Montana paid over $244 million in state Medicaid spending. This accounted for almost 32 percent of total Medicaid costs in Montana. In federal fiscal years 2009 and 2010 Montana's share percentage for total Medicaid costs decreased to 25 percent and 22 percent respectively.

System Implementation

Each state establishes its own eligibility standards, benefits package, payment rates and program administration under broad federal guidelines. DPHHS is responsible for managing Medicaid in Montana. To assist in the administration of Medicaid eligibility, DPHHS contracted with a third-party vendor to develop the Combined Healthcare Information and Montana Eligibility System (CHIMES) - Medicaid. This system replaces the Medicaid eligibility component of The Economic Assistance Management System (TEAMS) legacy application.

CHIMES – Medicaid was implemented in October 2009 at a cost of $13,364,201. The system is used by around 400 Medicaid eligibility examiners and supervisory staff

located in 51 offices throughout Montana. The system is designed to process enrollee information entered by eligibility examiners to assist in determining which Medicaid programs they are eligible for.

CHIMES – Medicaid was the first system DPHHS implemented as part of the overall CHIMES project to develop a new system for administering public assistance. When completed, CHIMES will consist of a combination of three separate systems:

- CHIMES – Medicaid
- CHIMES – SNAP (Supplemental Nutrition Assistance Program)
- CHIMES – TANF (Temporary Assistance for Needy Families)

While CHIMES – Medicaid has been implemented, development of the other two systems has not started. Once the other two systems have been implemented, the department plans to deactivate the legacy TEAMS application.

Audit Scope and Objectives

CHIMES – Medicaid is a complex system with processing dictated by a wide variety of both state and federal statutes and regulations. In addition, CHIMES – Medicaid manages over 80,000 client eligibility records and interfaces with 27 other systems. Because of this complexity, we limited scope to the following objectives:

1. Verify system access is limited to users with an identified business need.
2. Verify changes to the system follow standard change control procedures.
3. Verify the system is completely transferring data between interfaces.
4. Verify the system accurately determines program eligibility.
5. Verify data input controls ensure required data and data types are entered.
6. Verify system implementation followed industry standards for software development.

Methodology

To meet our objectives, we performed testing of CHIMES – Medicaid operations and controls including a combination of interviews of department staff, review of agency procedures and documentation, analysis of CHIMES – Medicaid data using computer assisted audit tools, and observations of CHIMES – Medicaid operations.

We evaluated the control environment using state policies, agency policies, federal law, and generally accepted government information technology standards established by the National Institute of Standards and Technology. The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office.

Summary

The following table provides an overall summary of the results of our audit.

Table 1
Summary of Audit Results

Control Areas	Audit Objectives	Testing Results
Input	#5 - required data entered	Pg 18 - recommendation
Processing	#4 - accurately determines eligibility	Pg 15 - conclusion
Output	#3 - complete transfer	Pg 18 - recommendation
Access	#1 - limited to business need	Pg 6-9 - recommendations
Change Management	#2 - follows standards	Pg 13-14 - conclusion and recommendations
Development	#6 - follows standards	Pg 3 - conclusion

Source: Compiled by the Legislative Audit Division.

Conclusion: System Controls Could Be Strengthened

As part of this audit, we verified CHIMES – Medicaid implementation followed industry standards for software development. We reviewed development contracts, system design standards, testing scripts and results, as well as other documents, in addition to interviews of staff and management. Development and implementation documentation suggests that, although testing could have been more thorough, DPHHS followed industry standards for the development and implementation of CHIMES – Medicaid. However, we identified other key areas where controls could be strengthened. Areas for improvement include user access, change management, and data integrity.

Chapter II – User Access

Introduction

In order to use the Combined Healthcare Information and Montana Eligibility System (CHIMES) – Medicaid, a user must be granted access. The Department of Public Health and Human Services' (DPHHS) primary method for securing CHIMES – Medicaid is to limit user access based on a policy of least privilege. Agency policy requires the data owner to determine if potential users need access and what level of access should be allowed based on their job duties. For CHIMES – Medicaid, the data owner is the Public Assistance Bureau. As an example, Quality Assurance Division staff would not be given any eligibility function access roles. In fact, there are seven eligibility function roles yet no single user has assigned access to all seven roles. In addition to examining compliance with these policies, we reviewed access to ensure it is limited to users with an identified business need.

Controlling Access Through Use of Roles

The National Institute of Standards and Technology (NIST) provides guidance on information technology. NIST recommends organizations manage information system accounts, establish a separation of duties, and employ the concept of least privilege. To control access based on specific duties, the department created 40 different access roles within CHIMES – Medicaid. For example, the Eligibility Worker and Eligibility Supervisor are two roles within eligibility functions, while central office has roles such as Trainer and Policy Specialist, and vendor roles include Help Desk and Developer roles. Each access role relies on supporting permissions delineating which screens and processes users can access and whether users can view, create, update, and/or delete information. In many instances, a single user can be assigned multiple access roles. To monitor access roles, the agency developed a spreadsheet referred to as the Security Matrix.

When CHIMES – Medicaid was initially implemented, department staff was responsible for managing and monitoring access roles. Early in the implementation process, the agency outsourced the management of roles to the vendor responsible for developing the system. Since user access is based on assigned roles, having the ability to maintain roles allows an individual the ability to grant themselves any level of access. Given the situation, there is potential risk the vendor, who is currently managing access roles, can modify these access roles without oversight or knowledge of the department. During the audit, we identified examples of this occurring; however, due to the extensive amount of data, audit testing did not include a review of all activities conducted as a result of this access.

As with any user, the vendor is assigned access roles. We reviewed the abilities of vendor roles and compared them to the Security Matrix to determine if they had been changed since the vendor began managing the roles. The roles we reviewed all had multiple changes to the screens or processes they could access. One of the vendor roles reviewed was changed from having a limited ability to modify data to having the ability to modify data in 484 of 489 available screens and processes. This means the vendor has access to functions outside normal system maintenance including the ability to determine Medicaid eligibility. We also noted roles other than the vendor roles had been changed. We reviewed the most common role assigned to eligibility examiners and identified 76 differences between the Security Matrix and actual assigned access. These changes to access roles were made without department knowledge.

Department Should More Actively Manage Access

While DPHHS reviews system access every six months, the process does not identify changes to the roles. As a result, there are multiple changes to roles that were not noted or updated in the Security Matrix. These changes resulted in different access than originally assigned, and some access is now excessive. Access management was assigned to the vendor due to a system problem. However, the department and vendor have addressed the system problem. As owners of the data and processes, DPHHS should reassume role management responsibility in order to maintain system security.

RECOMMENDATION #1

We recommend the Department of Public Health and Human Services:

A. *Reassume management of the system security through role management.*

B. *Update the Security Matrix to reflect actual role access.*

Monitoring Activity Associated With Privileged Access

One role that requires enhanced monitoring is "privileged" access. Privileged access allows a user to access screens or processes outside their regular duties or bypass system security or agency policy. CHIMES – Medicaid has one user role that meets the definition of privileged access: the statewide update role. We identified six users with this role. Five of the users are Central Office employees while the sixth user is from the Technology Services Division (TSD). With this role, these users have access to modify 358 of the 489 screens and processes, including those outside the Central Office and TSD functions.

The reason for assigning this role is to provide the user with the ability to correct data elements. Without formal monitoring or review, this level of access increases the risk of users making unapproved changes to client eligibility including adjusting eligibility characteristics to change a client's level of benefits. Industry standards suggest organizations manage user accounts. NIST suggests organizations that establish and administer privileged user access, also implement procedures to monitor and track activity associated with that access.

The department currently relies on a system process as a deterrent to improper user activity. Because users know when they change something it will be saved in the system's action history, the department believes the potential to review actions will prevent users from making unauthorized changes. Currently, the department performs some reviews of changes made to eligibility cases by users with privileged access. However, these reviews are informal with no defined schedule, are not documented, are not consistently applied to all users, and are performed by the users with the privileged access. As a result, the department's management of privileged access should be strengthened.

RECOMMENDATION #2

We recommend the Department of Public Health and Human Services:

A. *Document the business need for assigning privileged roles.*

B. *Establish formal monitoring of activities for all users with privileged access.*

C. *Ensure a segregation exists between users with privileged access and users monitoring role activities.*

Access Security

There are different strategies for controlling access to a system. Two of the most common methods are user-level security and the use of passwords. Access roles, described in the previous section, are a form of user-level security. This method coincides with the other method: use of passwords.

Passwords Not Being Fully Utilized

Passwords help secure user accounts by ensuring access to the system occurs only through assigned accounts. General system security requires users have unique usernames and passwords to log into a system. Montana has implemented policies to

guide statewide system operations. Statewide enterprise policy, requires passwords be changed by the user at their initial login and be changed at least every 60 days. During the audit, we noted CHIMES – Medicaid does not force users to change passwords at initial login.

We identified 91 users who have never changed their password in CHIMES – Medicaid. Further review noted 300 users have passwords older than 60 days. Of these, 243 passwords are more than 120 days old, and 217 passwords are more than 180 days old.

Without password security, control of unauthorized use of the system is minimized, which affects control over the intentional or unintentional modification, destruction, disclosure or misuse of data and resources. During our review, we noted DPHHS management believed CHIMES – Medicaid was forcing password changes at the initial login and every 60 days. However, based on our findings, this is not occurring.

RECOMMENDATION #3

We recommend the Department of Public Health and Human Services strengthen user-level security by ensuring compliance with statewide enterprise password policy.

Using the System to Monitor Access

CHIMES – Medicaid has a function to allow security officers to manage user's access. This function could be used to review a user's current access prior to granting further access to ensure conflicting or excessive access is not provided. It could also be used to ensure access is granted or removed, when the access was changed, and who made the change. However, current access of users are not always available for the security officer to view because user access does not update until a user logs into the system or, the user's access is completely removed and their account is closed. NIST recommends organizations manage user access including modifying, disabling, reviewing, and removing access. Without the ability to view current up-to-date access to the system, users can have excessive or conflicting duties due to difficulty in viewing current assignments when managing access.

Furthermore, the audit field used to track changes to a user's account, including when the access was changed and who made the change, also does not update until the next time the user logs in. Audit reviews noted the time stamp is inaccurate and the audit

fields do not update when the change actually occurred and who made the change. Instead, the system records the time and date of the next log-in. NIST recommends information systems use internal system clocks to generate time stamps at the point the auditable event occurs. NIST also recommends that an information system protects against an individual falsely denying having performed a particular action. Without correct system generated time stamps or identification of actual users associated with an auditable event, after-the-fact investigations cannot correctly identify the time of the event or the individual responsible.

During our review, department management said the system was designed to function this way in order to allow other processes to function properly, and due to limited funds. Agency documentation indicates this functionality was considered and a determination made to push its development to a later date due to project delays and associated cost. However, documentation shows the complexity of the change to be low with a minimal amount of hours required to add this security. DPHHS maintains a service contract for CHIMES–Medicaid that includes work necessary to correct CHIMES if not performing according to specification as well as work to add new functionality or change existing functionality. Based on the purpose of the service contract as well as the agency's representation of complexity and required hours, the department should be able to implement this functionality with no added costs.

RECOMMENDATION #4

We recommend the Department of Public Health and Human Services:

A. *Ensure current access information is available to the security officer.*

B. *Ensure documentation accurately depicts when a change occurred and who made the change.*

Chapter III – Change Management

Introduction

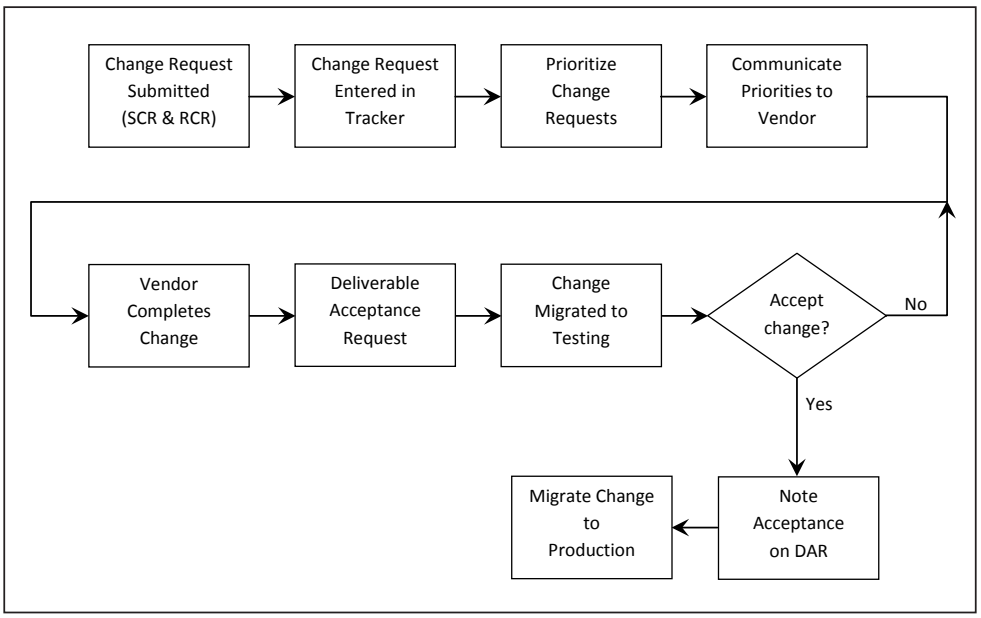
Information systems are generally a dynamic and fluidly changing environment. Data is modified and programming code updated to reflect the changing needs of an organization or to correct errors. However, because there are risks associated with any changes to data or programming code, an organization should mitigate risks by controlling changes. This occurs through a process called change management. The National Institute of Standards and Technology (NIST) provides guidance to organizations for managing information systems, and suggests organizations authorize, document, and control changes. We reviewed procedures in place for the Combined Healthcare Information and Montana Eligibility System (CHIMES) – Medicaid to ensure the Department of Public Health and Human Services (DPHHS) follows a standard change control procedure.

Data and Programming Code Changes

DPHHS change management includes controlling all changes made directly to the data and changes made to the underlying programming code dictating system processes. To track data changes, the system records who last updated a row of information in a table, as well as tracking every data change and who made the change for some specific information.

Changes to data or programming code are handled similarly. The following flow chart outlines the department's change management process, with more detail below the figure.

Figure 2
DPHHS Change Management Process



Source: Compiled by the Legislative Audit Division.

A System Change Request (SCR) is submitted for any new system changes while a Requirements Change Request (RCR) is submitted for any changes to existing system processes. All SCRs and RCRs are documented in Tracker, a separate computer application used to monitor the progress of changes to the system. The department holds weekly team meetings where change requests are prioritized. This prioritization is then communicated to the vendor.

Once the vendor completes a change request, they issue a Deliverable Acceptance Request (DAR) to DPHHS. A DAR is usually issued once a week and can include a single request or multiple SCR/RCRs. Since system implementation, 71 DARs have been issued each containing an average of 15 SCR/RCRs. The vendor then sends the file to the Department of Administration, State Information Technology Services Division (SITSD), for migration into a testing environment. DPHHS staff then test the changes to the system. Once testing is complete and DPHHS is satisfied with the changes, acceptance is noted on the DAR. Finally, the vendor sends the changes to SITSD for deployment to the CHIMES production environment.

Conclusion

Audit work determined the Department of Public Health and Human Services has implemented a change management process.

Migration Control Not Directly Managed by DPHHS

The CHIMES – Medicaid Service Level Agreement between DPHHS and SITSD requires the two organizations to work together to plan and coordinate upgrades and changes. It also requires DPHHS to document and test system changes to ensure they perform properly before implementation. Although DPHHS is testing and approving changes, it cannot guarantee only approved changes are being implemented. Once DPHHS has tested and accepted a change to the system, the vendor maintains control of migration to production. We noted direct contact between the vendor and SITSD when transmitting system changes. As a result, the vendor could submit unapproved data and programming code changes.

During our review, management said there is an expected procedure for migration to production. Only approved changes from the testing environment are to be migrated into production, which should not include receipt of a file from the vendor. This expected procedure reflects what industry best practices suggest. However, this procedure is not being followed, and files are being received directly from the vendor and migrated into production.

Recommendation #5

We recommend the Department of Public Health and Human Services migrate system changes directly from testing into production.

Server Access Could Be More Secure

System files and data are housed on servers maintained by SITSD under an agreement with DPHHS. The services provided under the agreement include maintaining system programming code. According to the Service Level Agreement, access to systems and databases will be strictly maintained and only appropriate levels will be authorized by the department and SITSD.

During our review, we noted SITSD is using nonsecure procedures to access CHIMES – Medicaid servers. System servers are accessed using shared usernames and passwords. Without using unique usernames and passwords to access servers, there is no accountability for data or system changes. This could result in unapproved modifications to the system.

While the Service Level Agreement requires SITSD to secure the servers, DPHHS owns the system and is responsible for ensuring the continued functionality of the system and the integrity of its data.

RECOMMENDATION #6

We recommend the Department of Public Health and Human Services ensure access to system servers is secure.

Chapter IV – Data Integrity

Introduction

Data integrity gives users assurance that the information in the system is trustworthy. Without data integrity, reporting and analysis will not provide users and decision-makers with accurate information nor allow the system to correctly determine eligibility. The Combined Healthcare Information and Montana Eligibility System (CHIMES) – Medicaid plays a key role in the management and administration of Medicaid eligibility. Given the amount of money distributed through the Medicaid program and the number of individuals who rely on the program for healthcare benefits, data integrity is critical. During this audit, we reviewed data integrity in several areas including data processing, input, and transfer.

How the System Processes Eligibility Data

We reviewed how the system processes eligibility data to ensure the accuracy of eligibility determinations. We selected a sample of program rules used to determine eligibility and verified these rules exist in the system. For those rules reviewed, we identified applicable language within the system. We also noted the system selects programs clients are eligible for based on internal logic. Eligibility examiners use the list of eligible Medicaid programs to determine final program enrollment. We noted client costs are consistently calculated and cannot be manually changed. Finally, we noted that when any change occurs with client data, the system reprocesses all of the data to redetermine program eligibility. Additionally, the department reviews a random sample of client records to ensure data processing is accurately determining eligibility.

Conclusion

We conclude the department has implemented controls to ensure the system is accurately processing data to assist in determining program eligibility.

Steps for Ensuring Data Accuracy

Industry standards recommend organizations report and classify system problems, including data anomalies and integrity issues. We reviewed several data fields within the system to verify data input controls are working as intended. During our review, we identified records with missing data in areas necessary for processing client eligibility. Areas tested are listed below, noting areas with missing data.

- Date of Application
- Client Last Name

- Client Date of Birth (missing data noted)
- Client Gender
- Social Security Number (missing data noted)
- Client Ethnicity
- Client Citizenship (missing data noted)

Inputting Data Into the System

We tested a sample of rules in the system that ensure adherence to program requirements. One such rule requires that anyone receiving various types of Medicaid have a Social Security Number (SSN). Department management said children under a year old could still receive Medicaid without a social security number. Our review of CHIMES – Medicaid data identified at least 22 clients over one year old that were issued Medicaid benefits but did not have a social security number entered in the system. Over $70,000 in medical benefits have been paid on behalf of these 22 clients. We asked DPHHS personnel about 5 of those 22 clients enrolled in the Family Medicaid program. Department staff said the issue was worker error or payments based on actual medical visits had not been issued on behalf of the clients.

Every client record within the system has a primary name listed, but can also have alias names. During our initial data analysis, we identified 1,826 records in CHIMES – Medicaid where the client's first and last names are the same. For example, a client's name would be; first name – SMITH, last name – SMITH or first name – WILLIAMS, last name – WILLIAMS. Subsequent reviews of the system ID number associated with the clients show all but one of the clients have this "double" name listed as an alias and not their primary. However, all records for the primary are also associated to the alias which could cause inaccurate reporting or confusion when reviewing the data within the system. For example, there are 13 different clients with "double" names SMITH, SMITH and WILLIAMS, WILLIAMS.

We also noted records that contained data inaccuracies. For example, Medicaid requires clients who can help cover medical costs to pay those costs prior to Medicaid payment (incurment). Once paid, client information is sent to the Medicaid Management Information System (MMIS) to pay remaining medical costs. However, we identified 10 clients where the system indicates they were transmitted to MMIS but the incurment costs had not been met. Subsequent review noted the client information was not actually sent to MMIS but the system erroneously marked them as having been sent.

Transferring Data Out of the System

There are currently 27 data interfaces with CHIMES – Medicaid. This includes both data being transmitted to and from the system. These interfaces transfer data through the use of data files created and monitored through Control M. Control M is an application designed to manage and run automated batch processes. Control M outputs a log file that identifies errors in the transfer process including dropped records or incomplete transfers due to data errors. Since Control M has been reviewed in prior audits of other systems, we concentrated our review to include comparisons of data between critical interfaces.

One critical interface we reviewed included the transfer of data between CHIMES – Medicaid and MMIS. While the majority of data appeared to completely transfer between the systems, we identified 21 records, within a single benefit month, of eligible Medicaid recipients in CHIMES – Medicaid whose eligibility was not reflected in MMIS. Department management stated the reason for the inaccuracies is due to missing data and unexpected data types. In these cases, incomplete or inaccurate data caused transfers to fail between the two systems.

Summary

DPHHS issues eligibility to an average 87,000 clients a year, so data integrity is important. While the number of exceptions we identified regarding missing or erroneous data were limited, data integrity issues do exist and can impact eligibility determination and decision-making. In the cases of the data anomalies identified in the data input and data transfer sections above, we determined DPHHS relies on staff and record reviewers to identify issues with data during normal use of the system. In addition, while the department reviews a random sample of client records, the number of cases is limited and the reviews relate to determining if eligibility examiners properly determined eligibility.

Department staff indicated they have implemented field edits to ensure most required data is entered before saving a client record. However, certain critical fields have exceptions and under certain circumstances are not required to be entered in the system. In these instances, it is possible for eligibility examiners to erroneously leave these fields blank. We did not identify any continuous testing to identify data anomalies to ensure data integrity. To help strengthen data integrity, DPHHS should develop a process to identify data anomalies within CHIMES – Medicaid. Based on our analysis, it does not appear this would create a significant burden in relation to time or costs.

RECOMMENDATION #7

We recommend the Department of Public Health and Human Services strengthen the current process to help identify missing and inaccurate data.

Department of Public Health and Human Services

Department Response

DEPARTMENT OF PUBLIC HEALTH AND HUMAN SERVICES

Brian Schweitzer
GOVERNOR

Anna Whiting Sorrell
DIRECTOR

STATE OF MONTANA

www.dphhs.mt.gov

February 7, 2011

Tori Hunthausen
Legislative Auditor
Legislative Audit Division
Room 160, State Capitol Building
PO Box 201705
Helena, Montana 59620-1705

Dear Ms. Hunthausen:

The Department of Public Health and Human Services has reviewed the Combined Healthcare Information and Montana Eligibility System for Medicaid Information Systems Audit (10DP-07) completed by the Legislative Audit Division. Our responses and corrective action plans for each recommendation are provided below.

RECOMMENDATION #1

A. DPHHS reassume management of the system security through role management.
B. DPHHS update the Security Matrix to reflect actual role access.

Response: Concur

Corrective Action:

A. The DPHHS HCSD PAB Security Officer was assigned complete management of the system security on December 14, 2010. Prior to this date, DPHHS managed the system security through the Change Process established for this project.

B. The Security Matrix has been updated to reflect current role access rules. Date/time stamped versions of the Security Matrix are available upon request. PAB will institute a quality assurance process that will involve a comparison of the Security Matrix with the Role Definition Summary web page to validate the implementation of changes to the Security Matrix within the CHIMES-Medicaid system.

Planned Completion Date: Completed.

RECOMMENDATION #2

A. DPHHS document the business need for assigning privileged roles.
B. DPHHS establish formal monitoring of activities for all users with privileged access.
C. DPHHS ensure a segregation exists between users with privileged access and users monitoring role activities.

Response: Concur

Corrective Action:

A. DPHHS will document the business need for assigning privileged roles and incorporate it into the PAB Central Office Policy.
B. DPHHS will establish a formal monitoring process of activities for all users with privileged update access and incorporate it into the PAB Central Office policy. The CHIMES system was designed and has the capability of retrieving system wide action history for each user to monitor all CHIMES activities.
C. DPHHS currently conducts random review of the activities performed by users with privileged update access. The supervisory personnel conducting the review are not involved in the activities being monitored. DPHHS will ensure segregation exists between users with privileged update access and users monitoring role activities and incorporate it into the PAB Central Office Policy.

Planned Completion Date: April 25th, 2011

RECOMMENDATION #3

A. DPHHS strengthen user-level security by ensuring compliance with statewide enterprise password policy.

Response: Concur.

Corrective Action:

A. The statewide enterprise policy was adopted by DPHHS on September 1, 2010. CHIMES-Medicaid has been updated to force password changes at the initial login and every 60 days. This change was implemented effective 10/13/2010. A System Change Request (SCR) has been submitted to add strong password functionality to CHIMES-Medicaid. The SCR is currently pending and will be prioritized through the DPHHS Change Management Process.

Planned Completion Date: Completed.

RECOMMENDATION #4

A. DPHHS ensure current access information is available to the security officer.
B. DPHHS ensure documentation accurately depicts when a change occurred and who made the changes.

Response: Concur.

Corrective Action:

A. DPHHS will ensure current access information is available to the HCSD PAB Security Officer through the use of the OM-300 process. The process for granting access to the CHIMES-Medicaid system begins when an OM-300A/B form is received by the HCSD PAB Security Officer who signs as the data owner approving roles in CHIMES–Medicaid that may be granted to the requestor. The HCSD PAB Security Officer retains copies of the OM300 DPHHS Security Access Request forms she signs to both grant and revoke rights to the CHIMES-Medicaid application. CHIMES-Medicaid access is not granted or revoked without a valid OM300 form. Additionally, the HCSD PAB security officer keeps a spreadsheet of all CHIMES users and their current access.

B. DPHHS will ensure documentation accurately depicts when a change occurred and who made the changes using the System Access Request Form (SARF) database as part of OM-300 tracking process.

When an OM-300 is completed, signed and approved by the HCSD PAB Security Officer indicating the roles a user may be granted, the form is sent to the DPHHS Security Operations Unit in the Network & Communications Bureau (NCB) of Technology Services Division (TSD). The Security Operations Unit then grants or revokes roles as directed by the HCSD PAB Security Officer on the form.

The DPHHS Security Operations Unit uses the System Access Request Form (SARF) database to electronically track all OM-300's received. Each system user has a profile in SARF with a record for any access they have been granted or that has been revoked. The SARF record for each user ID displays the date each access or delete action was requested, the supervisor and data owner who signed the form, the date the form was signed, the user requesting the access, the Security Unit staff member who performed the action, and the date the action was performed.

In addition to the OM-300 tracking process through SARF, the HCSD PAB Security Officer and the DPHHS Security Operations Unit conduct a bi-annual review to validate CHIMES-Medicaid users. This review involves the Security Unit electronically sending a cover letter explaining the review process and a spreadsheet listing all users and their roles to the HCSD PAB Security Officer for review. The HCSD PAB Security Officer then returns the spreadsheet, marking each

user/role on the spreadsheet as retain or delete. New forms are required to delete any roles/user indicated and, if necessary to add any roles.

Planned Completion Date: Completed.

RECOMMENDATION #5

A. DPHHS migrate system changes directly from testing to production.

Response: Concur.

Corrective Action:

A. DPHHS will modify its procedure for migrating files into production using industry best practices. In doing this, DPHHS will ensure that migration takes place directly from DPHHS approved files that have been successfully tested in the Test and QA environments.

Planned Completion Date: March 28th, 2011

RECOMMENDATION #6

A. DPHHS ensure access to system servers is secure.

Response: Concur.

Corrective Action:

A. DPHHS will work with the State Information Technology Services Division (SITSD) to incorporate a process in our Service Level Agreement (SLA) for CHIMES-Medicaid that ensures access to the system servers is secure.

Planned Completion Date: March 28th, 2011

RECOMMENDATION #7

A. DPHHS strengthen current process to help identify missing and inaccurate data.

Response: Concur.

Corrective Action:

A. While the CHIMES-Medicaid system is designed to notify the user during data entry of missing and inaccurate information through policy embedded in its business rules engine, the system allows certain fields such as SSN to remain blank in special circumstances that are dictated by policy. DPHHS will strengthen its current process to identify the special circumstances of missing and inaccurate data through additional training that emphasizes the need for all HCSD PAB staff to fully utilize existing reports which assist in the identification of missing and inaccurate data.

Planned Completion Date: April 25th, 2011

We appreciate the effort that your staff put into this audit and look forward to using these recommendations to continue improving operations and decrease risk within the Medicaid Eligibility System.

Sincerely,

Anna Whiting Sorrell

Director

cc. Ron Baldwin, Administrator Technology Services Division
Linda Snedigar, Administrator Human and Community Services Division
Marie Matthews, Audit Liaison